



## APPENDIX B

**Federal Reserve Banks  
Operating Circular No. 5**

### **ELECTRONIC ACCESS**

**Effective March 15, 2006**

**FEDERAL RESERVE BANKS  
OPERATING CIRCULAR NO. 5  
Effective March 15, 2006**

**ELECTRONIC ACCESS**

(Click CTRL + section or page number to go directly to the section)

<b>1.0 GENERAL .....</b>	<b>1</b>
1.1 INTRODUCTION.....	1
1.2 SERVICES ACCESSIBLE VIA ELECTRONIC CONNECTIONS.....	1
1.3 OTHER CIRCULARS; INSTITUTION'S AGREEMENT .....	2
1.4 INSTITUTION'S SECURITY OBLIGATIONS .....	3
1.5 PRIOR APPROVAL OR NOTICE REQUIREMENTS FOR ELECTRONIC CONNECTIONS .....	3
1.6 SERVICE PROVIDERS .....	3
<b>2.0 PARTICIPANT'S EQUIPMENT AND SOFTWARE.....</b>	<b>4</b>
<b>3.0 AVAILABLE ELECTRONIC CONNECTIONS .....</b>	<b>5</b>
<b>4.0 RESERVE BANK SUPPLIED OR DESIGNATED EQUIPMENT AND     SOFTWARE; WARRANTIES; DISCLAIMER OF WARRANTY .....</b>	<b>5</b>
4.1 EQUIPMENT DELIVERY, INSTALLATION, AND ALTERATIONS.....	5
4.2 ELECTRONIC CONNECTION TO NETWORK; SOFTWARE .....	5
4.3 SOFTWARE LICENSE .....	5
4.4 ELECTRONIC CONNECTION RESTRICTIONS.....	6
4.5 DISCLAIMER OF WARRANTY .....	6
4.6 UNAUTHORIZED DISCLOSURE OR USE OF SOFTWARE .....	7
4.7 RESERVE BANK'S VIRUS PROTECTION .....	7
4.8 INSTITUTION'S AND SERVICE PROVIDER'S VIRUS PROTECTION .....	8
<b>5.0 RISK AND LIABILITY IN USE OF ELECTRONIC CONNECTIONS.....</b>	<b>8</b>

5.1 RESPONSIBILITY FOR ACCESS CONTROL FEATURES .....	8
5.2 RESERVE BANK LIABILITY .....	9
5.3 COMPLIANCE WITH RESERVE BANK STANDARDS .....	9
5.4 CONFIDENTIALITY OF RESERVE BANK PROPRIETARY AND SECURITY-RELATED INFORMATION .....	10
5.5 MANAGEMENT OF ELECTRONIC CONNECTIONS .....	11
5.6 CONTINGENCY PLANS FOR DISRUPTION OF ELECTRONIC CONNECTIONS .....	11
6.0 FEES AND TAXES .....	12
6.1 ELECTRONIC CONNECTION FEES .....	12
6.2 OFF-LINE FEES DUE TO EQUIPMENT FAILURE .....	12
6.3 LIABILITY FOR TAXES .....	12
7.0 TERMINATION AND AMENDMENT .....	12
7.1 TERMINATING THE ELECTRONIC ACCESS AGREEMENT .....	12
7.2 RETURN OF RESERVE BANK SUPPLIED OR DESIGNATED EQUIPMENT AND SOFTWARE; SURVIVAL OF OBLIGATIONS .....	13
7.3 AMENDMENT OF CIRCULAR .....	13
8.0 FORUM, GOVERNING LAW AND TIME FOR ACTIONS .....	13
9.0 EFFECT OF THIS CIRCULAR ON PREVIOUS CIRCULAR .....	13

## 1.0 GENERAL

### 1.1 INTRODUCTION

This operating circular ("Circular") sets forth the terms under which an Institution may access certain services and applications provided by a Reserve Bank, and under which an Institution or its Service Provider may send certain data to or receive certain data from a Reserve Bank, by means of electronic connection(s).

For purposes of this Circular:

- (a) **Access Control Feature** means the software, encryption keys, logon identifications ("logon IDs"), passwords, pass phrases, digital certificates, Virtual Private Network ("VPN") devices, link encryptors, removable certificate storage devices ("tokens"), personal identification numbers ("PINs"), Secure Socket Layer ("SSL") technology, workstation configurations, workstation or network access restrictions (physical or logical), and other security measures used for access, authentication or authorization with regard to an Electronic Connection.
- (b) **Electronic Connection** refers to a communication facility used to exchange data between a Reserve Bank and an Institution or its Service Provider. The term includes but is not limited to an Internet, extranet, wireless, wide area network ("WAN"), local area network ("LAN"), or Frame Relay connection, and a connection for which access, authentication, or authorization is controlled by use of one or more Access Control Features.
- (c) **Institution** means (i) a depository institution as defined in Section 19(b) of the Federal Reserve Act (12 U.S.C. § 461(b)); (ii) a branch or agency of a foreign bank maintaining reserves under Section 7 of the International Banking Act of 1978 (12 U.S.C. § 347d, 3105); (iii) a department, agency, instrumentality, independent establishment, or office of the United States, or a wholly owned or controlled Government corporation; or (iv) another entity for which a Reserve Bank directly provides financial services.
- (d) **Reserve Bank** means any Federal Reserve Bank.
- (e) **Service Provider** means a person or entity, other than a Reserve Bank, that uses an Electronic Connection on behalf of an Institution.
- (f) **Software** means all software, including upgrades, modifications, applets and hypertext markup language ("HTML"), as well as any other code that resides on the Federal Reserve Banks' servers and/or mainframes that permits transactions to occur or data to be transferred between an Institution and a Reserve Bank and third party software that a Reserve Bank provides to an Institution for the purpose of accessing a Reserve Bank's services and/or applications.

### 1.2 SERVICES ACCESSIBLE VIA ELECTRONIC CONNECTIONS

Services which may be accessed using an Electronic Connection include, for example:

- a transfer of funds and/or securities;
- multilateral settlement service;
- commercial and/or governmental automated clearing house transactions;
- electronic presentment of checks;
- notification of nonpayment of checks;
- an order for cash and/or savings bonds;
- a bid for Treasury securities or Treasury investments;
- receipt of data related to services (such as check information, federal tax payment advices, and statements of account) sent by a Reserve Bank; and
- transmission of data related to services (such as check information and Treasury Tax and Loan ("TT&L") reports) to a Reserve Bank.

A Reserve Bank may from time to time offer other services and/or applications, such as transmission of statistical or financial reports or receipt of data related to those reports, using an Electronic Connection.

If an Institution submits statistical or regulatory reports to a Reserve Bank by an Electronic Connection, the Institution must use electronic submissions exclusively, unless it is unable to do so and it notifies the Reserve Bank prior to submitting data by other means. The Institution must maintain a hard copy duplicate of all required statistical or other bank regulatory data (such as FR 2900) that it submits electronically, unless, consistent with generally applicable revisions to the requirements for submitting the particular report, the Institution is no longer required to retain the hard copy. The hard copy must contain an official signature certifying that the data contained therein is correct, must be retained by the Institution for at least five years, and is subject to inspection by the Reserve Bank, by the Institution's primary regulator, and (for TT&L reports) by the Treasury Department.

### **1.3 OTHER CIRCULARS; INSTITUTION'S AGREEMENT**

Each Reserve Bank has issued a Circular identical to this one. In the event of any inconsistency between this Circular and any other Reserve Bank operating circular, agreement, or instruction governing particular types of transactions, such other operating circular, agreement or instruction controls. By accessing any services and/or applications from a Reserve Bank, or by sending data to or receiving data from a Reserve Bank, by means of any Electronic Connection, directly or through a Service Provider, an Institution agrees to the provisions of this Circular, including any Certification Practice Statement ("CPS"), as each may be amended from time to time, applicable to the Electronic Connection(s) that the Institution uses. The Institution also agrees to the provisions of any separate

agreement governing the use of a service, and agrees that any such agreement, including modifications and amendments thereto, may be posted and agreed to purely in electronic form. The current version of any CPS may be accessed at the Federal Reserve Financial Services Web site at [www.frbfinancialservices.org](http://www.frbfinancialservices.org), or such other location as a Reserve Bank may designate, the terms of which are incorporated in this Circular by reference.

#### **1.4 INSTITUTION'S SECURITY OBLIGATIONS**

The Institution agrees that complying with the security measures required by a Reserve Bank shall not relieve the Institution of its obligation and responsibility to exercise its own independent judgments about security and additional steps or procedures needed to prevent fraud, unauthorized access or other unauthorized use of an Electronic Connection with a Reserve Bank. Accordingly, an Institution agrees to take all additional commercially reasonable security measures in establishing an Electronic Connection with a Reserve Bank as circumstances may dictate over time; and further agrees to take all commercially reasonable security measures necessary to prevent disruption to the operations of any Reserve Bank's, and other Institutions', computers, networks, systems and software.

#### **1.5 PRIOR APPROVAL OR NOTICE REQUIREMENTS FOR ELECTRONIC CONNECTIONS**

A Reserve Bank's prior approval may be required before an Institution or a Service Provider uses an Electronic Connection to access any of the Reserve Bank's services and applications or to send any data to or receive any data from the Reserve Bank.

Additionally, an Institution must provide written notice before it uses a Service Provider, and an Institution or a Service Provider must provide prior written notice to the Reserve Bank before it:

- (a) shares the use of an Electronic Connection with another Institution or entity or,
- (b) sublicenses, assigns, delegates or transfers to a third party any of its rights, duties or obligations under this Circular.

The Reserve Bank reserves the right to reject any of the arrangements described in (a) or (b) above.

#### **1.6 SERVICE PROVIDERS**

By accessing any services and/or applications from a Reserve Bank, or by sending data to or receiving data from a Reserve Bank, by means of any Electronic Connection, a Service Provider agrees to the provisions of this Circular applicable to Service Providers. For purposes of the CPS, a Service Provider may be a Participant and/or a Subscriber, depending on its relationship with the Institution. The Reserve Bank reserves the right to require any Service Provider to agree in writing to additional terms and conditions, depending on the type of Electronic Connection and/or service the Service Provider is accessing on behalf of the Institution.

The provision of services by a Service Provider to an Institution shall in no way affect or diminish any obligation or duty of the Institution under this Circular or the provisions of any separate agreement governing the use of a particular Reserve Bank service. The Institution agrees that: (i) its Service Provider may be granted certain Access Control Features authorizing such Service Provider to use an Electronic Connection; (ii) its Service Provider will use those Access Control Features to act on behalf of the Institution; and (iii) its Service Provider may use the same Access Control Features to act on behalf of other Institutions that use the same Service Provider to access a Reserve Bank's computer systems. It is the responsibility of the Institution and its Service Provider to establish controls sufficient to ensure that the Service Provider properly segregates the data of the Institution from any data of other Institutions. The Reserve Banks are not required to take, and will not take, any measures to ensure that the Institution's data are properly segregated by its Service Provider. The Institution authorizes each Reserve Bank to rely on its Service Provider's identification of data as having been originated or authorized by the Institution. The sending or receiving of data by means of any Electronic Connection by a Service Provider purportedly on behalf of an Institution constitutes the sending or receiving of the data by the Institution for purposes of the Reserve Bank acting on such data.

Except to the extent prohibited by law or regulation, the Institution and the Service Provider shall defend, indemnify, and hold the Reserve Banks harmless against any liability, claim, loss, cost or expense, including, but not limited to, attorneys' fees and expenses of litigation, resulting from the Service Provider agency relationship or the acts or omissions of either the Institution or the Service Provider or their agents except, however, for any liability, claim, loss, cost or expense arising solely out of a Reserve Bank's failure to exercise ordinary care.

The Reserve Bank reserves the right, without prior notice, to terminate any Service Provider arrangement.

## **2.0 PARTICIPANT'S EQUIPMENT AND SOFTWARE**

An Institution is responsible for ensuring that its and its Service Provider's, if any, computer(s) and associated equipment and software comply with Reserve Bank requirements (which a Reserve Bank may change from time to time) and for maintaining its own equipment. The Reserve Banks reserve the right to approve or disapprove the use of an Institution's or its Service Provider's equipment and software, and/or to make recommendations regarding the equipment and software that the Institution uses. THE RESERVE BANKS DO NOT HAVE ANY OBLIGATION FOR, AND DO NOT MAKE ANY WARRANTY OR REPRESENTATION OF ANY KIND WITH RESPECT TO, ANY COMMUNICATION FACILITY, NETWORK, BROWSER, OPERATING SYSTEM, SERVER, OR ANY OTHER EQUIPMENT OR SOFTWARE NOT SUPPLIED, OWNED OR OPERATED BY A RESERVE BANK.

A Reserve Bank may, at its option, also specify third party vendors through which an Institution or its Service Provider must obtain equipment necessary for establishing and maintaining an Electronic Connection.

### **3.0 AVAILABLE ELECTRONIC CONNECTIONS**

An Institution or its Service Provider may choose from certain Electronic Connections that a Reserve Bank makes available and/or that a Reserve Bank permits to be used to connect to a Reserve Bank's services. A Reserve Bank reserves the right to specify the type of Electronic Connection necessary to support the volume and type of an Institution's transactions.

### **4.0 RESERVE BANK SUPPLIED OR DESIGNATED EQUIPMENT AND SOFTWARE; WARRANTIES; DISCLAIMER OF WARRANTY**

#### **4.1 EQUIPMENT DELIVERY, INSTALLATION, AND ALTERATIONS**

A Reserve Bank may, at its option, arrange for the delivery and/or installation of Reserve Bank supplied or designated equipment necessary for establishing an Electronic Connection.

Reserve Bank supplied or designated equipment may not be altered, encumbered, relocated, removed or transferred to a third party, except with the Reserve Bank's prior written approval. The Institution and its Service Provider, if any, are liable for any loss of and damage to Reserve Bank supplied or designated equipment, ordinary wear and tear excepted.

Unless otherwise agreed in writing, a Reserve Bank is not responsible for the delivery, installation, repair or alteration of any non-Reserve Bank supplied equipment, even if the Reserve Bank required that such equipment be used in order to establish an Electronic Connection to the Reserve Bank's computers.

#### **4.2 ELECTRONIC CONNECTION TO NETWORK; SOFTWARE**

The Reserve Banks require the use of specified Access Control Features to establish an Electronic Connection, and/or to permit access to certain services or applications over the connection. A Reserve Bank may provide, on request and where appropriate, either Computer Interface Protocol Specifications, product specifications, or Software (including documentation) to enable a connection to the Reserve Banks' network.

#### **4.3 SOFTWARE LICENSE**

In the event a Reserve Bank provides Software or access to Software, except as otherwise provided in a written agreement specifically referencing the Software, the Reserve Bank grants the Institution or its Service Provider, if any, a personal, nontransferable, nonexclusive license to use the Software solely for the purposes stated in this Circular and in compliance with applicable security procedures. The Reserve Bank warrants that it owns or has the right to license or sublicense the Software, and the Reserve Bank shall indemnify and hold the Institution and its Service Provider, if any, harmless from any loss or expense arising from any claim that the Software alone, and not in combination with any other party's products, software or activities, infringes a patent, copyright, trademark or other proprietary right of any third party, provided the Reserve Bank is given prompt written notice of the claim, has sole control of the defense of the claim and of any settlement negotiations, and the Institution and its Service Provider, if any, cooperate fully with the Reserve Bank in the defense and negotiations. In the



event of a claim that the Software infringes any third party proprietary right, the Reserve Bank reserves the right in its sole discretion to (a) replace the Software with a noninfringing product, (b) modify the Software to avoid the infringement, (c) obtain a license for the Institution to continue use of the Software, or (d) terminate the use of the Software.

#### **4.4 ELECTRONIC CONNECTION RESTRICTIONS**

An Institution or its Service Provider may not, except with a Reserve Bank's prior written consent:

- (a) situate any VPN device used in conjunction with an Electronic Connection in any location other than the Institution's or its Service Provider's premises within the United States or its territories\*;
- (b) modify, add to, translate, reverse assemble, reverse compile, decompile or otherwise attempt to derive the source code from any Software;
- (c) copy, sublicense or transfer the Software for any reason except that Software may be copied for back-up, testing or archival purposes, and all such copies shall include the Reserve Bank's and any third party's copyright, trademark and proprietary notices externally in the distribution medium and internally in machine-readable form; or,
- (d) remove any copyright or trademark notice contained in the Software.

Use of an Electronic Connection from outside of the U.S. and its territories is permissible only in accordance with the Reserve Banks' policies and procedures pertaining to foreign access. Institution acknowledges and understands that it and its Service Provider, if any, will be required to agree to additional terms and conditions governing any regular and on-going foreign access (including contingency arrangements) prior to such use of an Electronic Connection.

#### **4.5 DISCLAIMER OF WARRANTY**

Reserve Bank supplied or designated equipment and Software (including documentation), and any Access Control Feature, Electronic Connection, recommendation, security procedure, operating instruction, user manual, guideline and specification for an Electronic Connection that a Reserve Bank specifies, are furnished strictly on an "as-is" basis. The Reserve Banks do not warrant or represent that operation of any Reserve Bank supplied or designated equipment or Software or use of an Electronic Connection or Access Control Feature will meet an Institution's or its Service Provider's planned applications, that Reserve Bank supplied or designated equipment or Software will be compatible with an Institution's or its Service Provider's equipment, or that any defect in Reserve Bank supplied or designated equipment or Software can be corrected. The Reserve Banks do not warrant or represent that use of an Electronic Connection, regardless of whether used in conjunction with any Access Control Features and/or in compliance with any recommendations, security procedures, operating instructions, user manuals, guidelines, other documentation, and specifications for an Electronic Connection that a Reserve

---

\* Puerto Rico, the U.S. Virgin Islands, American Samoa, Guam and the Northern Mariana Islands.

Bank specifies, will be uninterrupted, free from interception, timely, secure, or error free.

A Reserve Bank's sole obligation in the event of a malfunction in Reserve Bank supplied equipment or Software is to provide a remedy in the form of either providing reasonable assistance in resolving problems or replacing defective or damaged equipment or Software that: (1) an Institution or its Service Provider returns to the Reserve Bank or (2) about which an Institution or its Service Provider informs the Reserve Bank. The Reserve Bank shall have sole authority to select the form of the remedy to satisfy that obligation, if any.

A Reserve Bank shall have no obligation for equipment or software that is purchased by the Institution or its Service Provider from a third party vendor, even if the Reserve Bank requires the use of that equipment or software or arranges for the purchase from said vendor.

THE OBLIGATIONS AND THE WARRANTY SET FORTH IN THIS PARAGRAPH AND IN PARAGRAPH 4.3 ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY OTHER WARRANTY ARISING BY STATUTE OR FROM A COURSE OF DEALING OR USAGE OF TRADE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY A RESERVE BANK SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THE RESERVE BANKS' OBLIGATIONS.

#### **4.6 UNAUTHORIZED DISCLOSURE OR USE OF SOFTWARE**

Software includes trade secrets and proprietary information of the Reserve Banks and others, which may be copyrighted or patented, and must be handled in accordance with the requirements applicable to Confidential Information as set forth in Paragraph 5.4.

#### **4.7 RESERVE BANK'S VIRUS PROTECTION**

The Reserve Banks provide Software either on diskettes, CD-ROMS or other electronic media or through data transmission facilities. The media have been duplicated or sent by the Reserve Banks or by outside suppliers whom the Reserve Banks believe use equipment protected by commercially reasonable technology to prevent the introduction of viruses, malicious code and other defects. The Reserve Banks test random samples of diskettes and CD-ROMS obtained from vendors, using virus-detection software that the Reserve Banks believe is commercially reasonable. However, it is not commercially feasible for the Reserve Banks to test all such diskettes, CD-ROMS and other electronic media, and the virus-detection software may not detect all viruses, malicious code or other defects. Reserve Bank data transmission facilities also are protected by what the Reserve Banks believe is commercially reasonable technology to prevent the introduction of viruses, malicious code and other defects.

#### **4.8 INSTITUTION'S AND SERVICE PROVIDER'S VIRUS PROTECTION**

The Institution and its Service Provider, if any, agree to take all commercially reasonable precautions to prevent the introduction of a computer virus, malicious code or other defect that might disrupt the operations of a Reserve Bank's, or other Institutions' or Service Providers', computers or software, including the installation, operation and proper configuration of commercially reasonable anti-virus software. Certain Software that a Reserve Bank supplies may not be compatible with all types of commercial anti-virus software. Accordingly, an Institution or its Service Provider may need to use an alternative type of commercial anti-virus software on certain computers that contain Access Control Feature(s) or that are otherwise engaged in Electronic Connection(s) with a Reserve Bank.

### **5.0 RISK AND LIABILITY IN USE OF ELECTRONIC CONNECTIONS**

#### **5.1 RESPONSIBILITY FOR ACCESS CONTROL FEATURES**

An Institution and its Service Provider, if any:

- (a) must use all Access Control Features specified by a Reserve Bank, but may use any Access Control Features supplied by a Reserve Bank or by a vendor specified by a Reserve Bank only for authorized access to a Reserve Bank's services and/or applications;
- (b) acknowledge that their Electronic Connection(s) and the Access Control Features can be used to originate funds transfer messages, other value transfer messages and non-value messages;
- (c) except as otherwise provided in this Circular, assume sole responsibility and the entire risk of use and operation of their Electronic Connection(s) and the Access Control Features;
- (d) are responsible for unauthorized physical and network access to their Electronic Connection(s) and applicable Access Control Features;
- (e) are responsible for establishing, instituting and enforcing policies and procedures for controlling, detecting and preventing unauthorized physical and network access to all applicable Access Control Features, and for immediately contacting the Reserve Bank if they have a reasonable basis to suspect that any applicable Access Control Feature is missing, has been compromised or shows evidence of tampering.

Any Reserve Bank may act on any message that it receives through an Electronic Connection that the Reserve Bank authenticates as an Institution's directly (or an Institution's through its Service Provider, where applicable), using such technical protocols and procedures as the Reserve Bank shall establish in its sole discretion as if the message consisted of a written instruction bearing the manual signature of one of the Institution's duly authorized officers.

## **5.2 RESERVE BANK LIABILITY**

The Reserve Banks are not liable for loss or damage resulting from a problem beyond their reasonable control. This includes, but is not limited to, (a) loss or damage resulting from any delay, error or omission in the transmission of any message to or from an Institution or its Service Provider; (b) alteration of any data, instruction or notice sent to or from a Reserve Bank through an Electronic Connection; (c) any third party's interception and/or use of any data conveyed using an Electronic Connection; (d) the services provided by an internet service provider; (e) a virus, malicious code or other defect received from or introduced by any entity other than a Reserve Bank; (f) or technology provided by a Reserve Bank if the technology was not developed by a Reserve Bank, even if the Reserve Bank requires the use of such technology. Additionally, Reserve Banks are not liable for loss or damage resulting from unavailability of an Electronic Connection due to security or other concerns which the Reserve Banks, in their sole discretion, may conclude justify making such Electronic Connection unavailable, or from strikes, labor disputes or civil unrest, acts of war, riots, acts of terrorism, acts of God or acts of nature.

Further, the Reserve Banks are not liable for any loss or damage arising from an Institution's or its Service Provider's use of any Access Control Feature, or from a third party's reliance on any Access Control Feature, for any purposes other than those expressly authorized by a Reserve Bank. The Reserve Banks are not liable for any loss or damage arising from the theft or compromise of a private key or the password that protects a private key, whether detected or undetected, the storage of any private keys on an Institution's or its Service Provider's computer hard drive(s) or other storage device, or any loss caused by a third party's use or duplication of a private key.

Except as provided in Paragraph 4.3 of this Circular, a Reserve Bank shall be liable only to the Institution, only for losses that result from failure by the Reserve Bank or its employees to exercise ordinary care or act in good faith in providing the Electronic Connection, and only up to the amount of any fees paid to the Reserve Bank for the relevant Electronic Connection during the one month period immediately prior to the transaction or occurrence giving rise to the liability. In no event shall the Reserve Bank be liable for special, incidental, or consequential damages, even if such damages were foreseeable at the time of the Reserve Bank's failure to exercise ordinary care or act in good faith.

Except for a liability, claim or loss arising exclusively from the Reserve Bank's failure to exercise ordinary care or act in good faith in providing an Electronic Connection, and except to the extent prohibited by law or regulation, the Institution shall indemnify, defend, and hold harmless the Reserve Bank with respect to any liability, claim or loss, whether alleged by the Institution, any customer of the Institution, its Service Provider or any third party, arising in connection with the use by the Institution (or its Service Provider or other agents) of the Electronic Connection. This indemnification shall survive the termination of access provided under this Agreement.

## **5.3 COMPLIANCE WITH RESERVE BANK STANDARDS**

An Institution and its Service Providers, if any, agree to use the Access Control Features, and agree to conform to the security procedures, operating

instructions, guidelines, and specifications applicable to an Electronic Connection that a Reserve Bank specifies from time to time, including the need for the Institution and its Service Provider, if any, to exercise their own independent judgment about the adequacy of existing security measures. Notwithstanding the above, the Institution and its Service Providers, if any, are required and agree to implement appropriate physical security to protect the Access Control Features, Software, computer(s) and any associated equipment that are used to exchange data with a Reserve Bank from unauthorized use. THE RESERVE BANKS MAKE NO WARRANTIES WITH RESPECT TO THE FOREGOING OR OTHERWISE IN CONNECTION WITH THE USE OF AN ELECTRONIC CONNECTION, EXCEPT AS EXPRESSLY SET FORTH IN THIS CIRCULAR.

#### **5.4 CONFIDENTIALITY OF RESERVE BANK PROPRIETARY AND SECURITY-RELATED INFORMATION**

“Confidential Information” shall include all information, provided in writing, electronically or orally, which is designated by Reserve Bank herein or by other means as “Confidential.” **All security-related information, including information regarding Access Control Features and security procedures, whether or not it is labeled as “Confidential,” is hereby designated as “Confidential,”** unless a Reserve Bank makes any such information generally available to the public (i.e., places it on its unrestricted public Web site or otherwise publishes it to the general public). Confidential Information contains trade secrets, proprietary information or security information of Reserve Banks or others. Unauthorized disclosure of Confidential Information likely would cause a Reserve Bank immediate and irreparable damage for which there may be no adequate remedy at law.

The Institution and its Service Provider, if any, agree to take all reasonable measures to protect and ensure the secrecy of and affirmatively avoid disclosure and unauthorized use of Confidential Information. Without limiting the foregoing, the Institution and its Service Provider, if any, shall protect the Confidential Information with at least the same degree of care that the Institution uses to protect its own highly confidential information and comply with all handling instructions that are provided with the Confidential Information. The Institution and its Service Provider, if any, are responsible for destroying or returning any Confidential Information to Reserve Bank upon the request of Reserve Bank or when the Confidential Information is no longer needed.

The Institution and its Service Provider, if any, shall disclose the Confidential Information to their employees or third parties only on a “need to know” basis. The Institution and its Service Provider, if any, shall maintain a written record of all third parties to whom Confidential Information is disclosed (indicating the recipient, date and description of content of the disclosure), and shall provide such record to the Reserve Bank upon request. The Institution and its Service Provider must take all necessary steps to enforce the obligations of Paragraph 5.4 with their employees. Before disclosure to any third party, the Institution and its Service Provider, if any, must have a written agreement with such party sufficient to require that party to treat the Confidential Information in accordance with Paragraph 5.4. The Institution and its Service Provider, if any, are liable for any unauthorized disclosure of Confidential Information by any of their employees or third parties to whom they have disclosed Confidential Information.

In the event the Institution or its Service Provider become aware of any unauthorized disclosure or use of the Confidential Information, the Institution or Service Provider must immediately notify Reserve Bank of the unauthorized disclosure or use, and must use their best efforts to prevent further unauthorized disclosure or use. Such notification must be by telephone, with written confirmation to Reserve Bank.

An Institution or its Service Provider must notify the Reserve Bank(s) with which it has an Electronic Connection immediately by telephone, with written confirmation, of any suspected fraud, infringement, or security breach relating to the Electronic Connection(s).

## **5.5 MANAGEMENT OF ELECTRONIC CONNECTIONS**

- (a) An Institution or its Service Provider must manage its Electronic Connection(s) so as to permit the Reserve Banks to send data to the Institution or the Service Provider, and to permit the Institution or the Service Provider to receive data from the Reserve Banks, on a timely basis throughout the day. A Reserve Bank is not responsible for any delay in sending data (or for notifying any party of such a delay), if the delay results from the Institution's or its Service Provider's failure to so manage its connection(s), or from any cause other than the Reserve Bank's failure to exercise ordinary care or to act in good faith. The Reserve Bank's records shall be determinative of when data has been received by a Reserve Bank or when a Reserve Bank sends data to, or makes it retrievable by, the Institution or its Service Provider.
- (b) An Institution and its Service Provider, if any, are responsible for reviewing the current Reserve Bank hardware, software and connection requirements ("System Requirements") on a regular basis and updating their operating systems accordingly. A Reserve Bank shall make best efforts to provide notice (which may be in electronic form) of changes to the System Requirements. An Institution or its Service Provider must also update in a timely manner all applicable workstation operating systems, anti-virus software and any other software used in connection with or comprising the Institution's or its Service Provider's Electronic Connections. The Reserve Banks shall not be responsible or liable in any manner for any loss or damage to an Institution or its Service Provider that could have been prevented had an update been installed when such update was made available by the applicable vendor. The Reserve Banks shall also not be responsible or liable in any manner for any loss or damage caused directly or indirectly by the installation of any such update whether or not the update was directly provided by a Reserve Bank.

## **5.6 CONTINGENCY PLANS FOR DISRUPTION OF ELECTRONIC CONNECTIONS**

Problems with hardware, software, or data transmission may on occasion delay or prevent a Reserve Bank from sending or receiving payments or other data electronically. Accordingly, an Institution and its Service Provider, if any, should be prepared to send or receive payments or other data by other means.

An Institution and its Service Provider agree to establish and regularly test business continuity and disaster recovery plans for use in the event of loss of a single or group of Electronic Connections to a Reserve Bank.

## **6.0 FEES AND TAXES**

### **6.1. ELECTRONIC CONNECTION FEES**

A Reserve Bank's fees relating to Electronic Connections (including, for example, installation support and training) are published separately and are subject to change on thirty (30) calendar days' prior notice. A Reserve Bank charges these fees to the Institution's (or its correspondent's) account on a Reserve Bank's books. By designating a Service Provider, an Institution agrees that the Service Provider may be billed directly by the Reserve Bank for any fees related to the Service Provider's Electronic Connection. Notwithstanding any such direct billing, the Institution shall remain liable for any unpaid fees.

### **6.2 OFF-LINE FEES DUE TO EQUIPMENT FAILURE**

If, because of a failure of an Institution's or its Service Provider's equipment, either a Reserve Bank or the Institution reverts to an off-line procedure, the Reserve Bank may charge off-line fees to the Institution.

### **6.3 LIABILITY FOR TAXES**

An Institution and its Service Provider, if any, are liable for the payment of any taxes, however designated, levied on its possession or use of equipment, services and/or applications or Software a Reserve Bank has supplied, including, without limitation, state and local sales, use, value-added and property taxes.

## **7.0 TERMINATION AND AMENDMENT**

### **7.1 TERMINATING THE ELECTRONIC ACCESS AGREEMENT**

An Institution may terminate its agreement to use Reserve Bank services and/or applications through an Electronic Connection and its agreement to the terms of this Circular by giving not less than thirty (30) calendar days' prior written notice to the Reserve Bank(s) with which it has Electronic Connections. A Reserve Bank may terminate an Institution's or its Service Provider's authority to use an Electronic Connection on similar notice. In addition, a Reserve Bank immediately may terminate an Institution's or its Service Provider's Electronic Connection if the Reserve Bank, in its sole discretion, determines that continued use of the Electronic Connection poses a risk to the Reserve Bank or others, or the Reserve Bank believes that the Institution or its Service Provider is in violation of this Circular.

The Reserve Bank, in its discretion, may restore the Electronic Connection when the Reserve Bank deems appropriate.

An Institution and its Service Provider, if any, are solely responsible for the proper operation of their electronic information systems. A Reserve Bank in its discretion may suspend or disconnect an Electronic Connection in the event that such access to the Reserve Bank's systems generates error conditions, causes

denials or disruptions of the Reserve Bank's systems, or appears to have been compromised with respect to information security or integrity. In the event of any such suspension or disconnection, the Reserve Bank and the Institution and its Service Provider, if any, will cooperate to investigate, identify, and correct the problem or problems affecting access to the Reserve Bank's systems.

## **7.2 RETURN OF RESERVE BANK SUPPLIED OR DESIGNATED EQUIPMENT AND SOFTWARE; SURVIVAL OF OBLIGATIONS**

Upon termination, an Institution and its Service Provider, if any, promptly must: (a) disable (by removing the battery or otherwise) any encryption card, or other card that supports encryption and communication, but only after the workstation has been disconnected from production network connections; (b) return all Reserve Bank supplied or designated equipment (or properly dispose of it, if a Reserve Bank authorizes it to do so); (c) destroy or return, as required herein any Software and Confidential information provided to the Institution and its Service Provider, if any; (d) delete as required herein any installed copies of such Software or saved copies of Confidential information; and (e) upon request of a Reserve Bank, provide written certification that all relevant Software and Confidential information has been destroyed and deleted. Notwithstanding the foregoing, the Reserve Bank retains the right to require that an Institution and its Service Provider, if any, promptly return all relevant Software, hardware and Confidential information upon termination. The Institution's and its Service Provider's obligations pertaining to confidentiality, nondisclosure and cooperation with a Reserve Bank's defense of any Software infringement claim survive any termination of the Institution's and its Service Provider's agreement to this Circular.

## **7.3 AMENDMENT OF CIRCULAR**

The Reserve Banks may amend this Circular at any time without prior notice. Any amendment applies immediately upon the effective date of the amendment.

## **8.0 FORUM, GOVERNING LAW AND TIME FOR ACTIONS**

The exclusive forum for any action involving a Reserve Bank for that Reserve Bank's acts or omissions arising under this Circular is in the United States District Court and Division where the head office of the Reserve Bank that committed the alleged act or omission is located and the Institution and its Service Provider, if any, hereby submit to the exclusive jurisdiction of such court. No action or claim relating to this Circular may be instituted more than one year after the event giving rise to such action or claim. This Circular is governed by Federal law and, to the extent not inconsistent therewith, the law of the State in which said Reserve Bank's head office is located, excluding that State's law regarding conflicts of law.

## **9.0 EFFECT OF THIS CIRCULAR ON PREVIOUS CIRCULAR**

This Circular amends and supersedes all prior versions of Reserve Bank Operating Circular 5, and shall be effective on March 15, 2006.